

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034190 A2

- (51) International Patent Classification⁷: **G06F**
- (21) International Application Number:
PCT/US2003/031333
- (22) International Filing Date: 2 October 2003 (02.10.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/416,185 4 October 2002 (04.10.2002) US
- (71) Applicant (for all designated States except US): **WOOD-STOCK SYSTEMS, LLC** [US/US]; 36 E. 67th Street, New York, NY 10021 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **HOFFMAN, James**

[US/US]; 18 Northwoods Road, Woodstock, NY 12498 (US). **FRISKEL, James** [US/US]; 3221 South Atlantic Avenue #704, Cocoa Beach, FL 32931 (US).

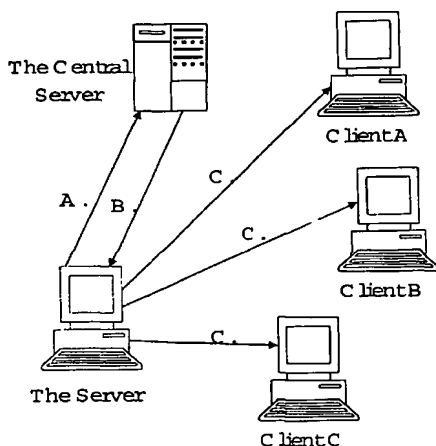
(74) Agents: **LEMACK, Kevin, S.** et al.; Nields & Lemack, Suite 7, 176 E. Main Street, Westboro, MA 01581 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: METHOD FOR RUNNING SERVERS BEHIND FIREWALLS, ROUTERS, PROXY SERVERS AND NETWORK ADDRESS TRANSLATION SOFTWARE AND DEVICES



(57) Abstract: The present invention provides a system and method for automatically and securely enabling a server to be accessed by systems and devices under conditions where it would otherwise be inaccessible. Servers maintain higher levels of security as listening ports are not utilized in the invention. The methods described allow access between devices, even in the presence of firewalls, proxy servers and NAT devices.

- A. The server, behind a firewall, router, proxy server or NAT device accesses the Central Server.
- B. The server obtains the IP address of all authorized Clients from the Central Server.
- C. The server then makes a connection with all of the Clients (shown as Clients A, B, and C which are merely representative of any number of Clients).



SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *without international search report and to be republished upon receipt of that report*

**METHOD FOR RUNNING SERVERS BEHIND FIREWALLS, ROUTERS, PROXY
SERVERS AND NETWORK ADDRESS TRANSLATION SOFTWARE AND DEVICES**

This application claims the benefit of domestic priority based on provisional application, 60/416,185, filed October 4, 2002, entitled "Method for Running Servers Behind Firewalls, Routers, Proxy Servers and Network Address Translation Software and Devices", submitted by Woodstock Systems, LLC, f/k/a MediaStor, LLC, the disclosure of which is hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates to computer networks, and in particular the ability of a server to access a receiving communications port despite certain system/infrastructure issues that might otherwise prevent such access.

BACKGROUND OF THE INVENTION

With the advances of computer information systems, individuals and businesses around the world regularly provide remote access to a computer or device. Increasingly, this access is complicated by firewalls, routers, proxy servers and NAT (Network Address Translation) mediation. These network devices and software, either by design or unintentionally, block or reassign ports and Internet Protocol (IP) addresses, thereby preventing an external computer or device from accessing a computer or device that is on a network equipped with such devices or software.

A typical Web server application or device serves data to a computer connected to the server's "Listening port". This port must be accessible to the server, or the server would never receive the computer's request. Firewalls, routers, proxy servers and NAT devices can all impair or

eliminate a server's ability to locate an accessible port. This creates significant problems for businesses and consumers. The current solution to these problems involves extremely complicated configuration setting of the blocking firewall, router, proxy server or NAT device, and in many cases, a solution does not currently exist. The need for simple methods that will automatically and securely provide this type of access is critical for many current and future uses, both at work and at home.

More specifically, in conventional computer networks today, computers require a port to be semi-permanently configured to allow incoming traffic that is not in direct conjunction with a previous outbound communication to pass through. These ports are referred to as "listening ports" and allow computers to detect network communication that is intended for them. These ports are publicly visible and any other computer on the network can attach to these ports. While this is intended to allow a simple method of having 2 computers, previously unknown to each other, communicate; there are a number of drawbacks in this scheme. Publicly visible ports are vulnerable to attack by other (e.g. unauthorized) computers. Denial of Service attacks, where another computer constantly sends messages to the computer in an attempt to deplete its resources, are one such problem. Another security issue is "worm-like" software trolling IP addresses on the network looking for public listening ports to attack. To counteract these attacks, a number of security protocols and devices have been devised, such as firewalls. These devices reduce the risk of such an attack, but make the allowable access to a computer more difficult. For example, a firewall may allow all incoming traffic or restrict it to allow only certain IP addresses to access the computer

network behind it. A set of users may wish to set up a share group, where they can view certain files on each other's computers. When an unknown computer, wishing to join the share group with no malicious intent, attempts to access a computer behind the firewall to access some shareable files, that access will be denied by the firewall. This makes the process of creating share groups very difficult, as the firewall would need to be reconfigured each time a new member joins the share group. Similarly, Network Translation devices (NAT devices) address the security issue by opening the port only for one computer to communicate. Present systems force users to choose between tight security with minimal or difficult sharing capabilities, or full sharing capabilities with minimal or no security.

SUMMARY OF THE INVENTION

The present invention overcomes the current shortcomings in the prior art by providing a system and method for automatically and securely enabling a server to be accessed by systems and devices under conditions where it would otherwise be inaccessible, or where accessibility would be difficult. The present invention has particular applicability in connection with the Personal Digital Server ("PDS"), a computer application for the storage, updating, management and sharing of all types of digital media files, including audio, video, images and documents, irrespective of their format. A Patent Application for PDS, entitled "Personal Digital Server™ (PDS™)", application number PCT/US 02/41403 was filed by Woodstock Systems, LLC, f/k/a MediaStor, LLC on December 24, 2002 and is hereby incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates an exemplary embodiment of a computer network system and a method for setting up a computer server as a non-listening server according to the present invention;

Figure 2 illustrates an exemplary embodiment of initiation of client request to a server in the "Non Listening Server" mode in the computer network system of Figure 1 according to the present invention;

Figure 3 illustrates an exemplary embodiment of the status of the computer network system shown in Figure 1 when the server is acting as a "Just-in-Time Listening Server" in waiting mode according to the present invention; and

Figure 4 illustrates an exemplary embodiment of a client request when the server is acting as a "Just-In-Time Listening Server".

DETAILED DESCRIPTION OF THE INVENTION

The present invention allows a server application or device to share files and other media with other computers in a secure and simple method. Two approaches to this are disclosed. One is referred to as "just-in-time-listening (JITL)" mode. The second approach, known as "Non-Listening Server (NLS)" mode can be employed particularly when tighter security constraints are desired.

The Non-Listening Server (NLS)

A software application can operate on a server without a publicly visible "listening" port when utilizing the Non-Listening Server (NLS) method. This method is shown in Figure 1. In Step A, the server 10 securely connects itself to a

central administrative node 20. The central server preferably always has a listening node. The security of the central administrative node is maintained preferably by limiting the software applications resident on the node to a minimum, most preferably to only this application. Access to the central administrative node 20 can be achieved by methods well known in the art. For example, a fixed IP address may be used, or more preferably, a domain name, such as for example <http://registration.WoodstockSystems.com>, the identity of which server 10 is aware. The server can be located behind a firewall, proxy server, router or Network Address Translation device. Since the server is the device initiating the transaction, it is able to access the central node without issue. In Step B, in response to a request by the connected server, the central administrative node supplies the current IP address of users, systems and devices (collectively, "Clients") that are authorized to access that specific server. Since the list of authorized users can be a dynamic entity, this list can be continuously updated at the server. This can be done in a number of ways, including having the server query the central administrative node at regular intervals, having the central node notify the server of any changes to the list, or maintaining a persistent connection to the central node and receiving these updates in real time. Other suitable update methods are available and are well known in the art.

In the "Non Listening Server" mode, the server does not have any open listening ports; therefore clients are unable to connect directly to the server. Instead, as shown in step C, the server securely connects itself directly to each of the authorized Clients, 30a, 30b and 30c, as identified by the central administrative node, via its own outbound

messaging. It will be understood by those skilled in the art that although three authorized clients are shown, there could be any number of clients without departing from the spirit and scope of the preset invention. In this way, a secure communications path is established between the server and each of its authorized clients.

Figure 2 illustrates, in step D, the scenario where a client 30b can request specific data from the server 10 using the open connection established previously by the server in Figure 1. In step E, the server 10 can then serve the data to the requesting Client 30b using the open connection. Steps D and E can then be repeated each time that the client requests information from the server.

In this embodiment, the server never opens up an externally available 'listening' port, so the security risk of rogue software targeting TCP/IP 'listening' ports is eliminated. All communication occurs during sessions that that server itself initiated. This eliminates the possibility of a denial-of-service attack on the server and also eliminates the possibility of any 'worm-like' software trolling IP addresses for 'listening' ports.

The server in Non-Listening Server (NLS) mode can operate behind the most stringent firewalls when it makes an outside connection to the Internet, as shown in Figure 1. However, it is noted in this method that a server running in NLS mode cannot communicate with Clients that are also behind a firewall.

Additional levels of security can be added to the NLS scenario via encryption technology if desired. For example, the messages exchanged in the NLS mode can be encrypted,

using algorithms and technologies that are known by those skilled in the art.

The Just-In-Time Listening (JITL)

The "non-listening" server mode provides superior security against attacks, since the server never opens a publicly visible port. However, the NLS mode cannot function properly if the clients reside behind a firewall. The Just-In-Time Listening method extends capabilities of the "non-listening" server method to operate in environments where both the server and its Client are behind firewalls or in environments where the Client's information may need to change dynamically. This is accomplished using essentially the same techniques as in the NLS mode, with one exception. Instead of never opening up a publicly visible port to listen, the server opens a temporary listening port for only the time necessary to receive a short encrypted reply from an authorized Client. This temporary listening port will only accept a connection from the one Client that it is waiting on, and it will only wait for a short period of time, preferably under one second. If any other TCP/IP address connects to it during the time the port is open, it will be immediately rejected, the port is closed and the listening halts. If the connection is not properly authorized, the connection is immediately dropped and listening halts. In addition, if the connection is properly authorized, any listening beyond the necessary establishment of a connection also immediately halts. In other words, the connection only 'listens' long enough to receive the one request it is awaiting, and immediately stops 'listening' after establishing that connection or after an extremely brief

timeout period. The coordination of this communication between the server and Client is accomplished through their communication with a central administrative node as illustrated in Figures 3 and 4.

Referring to Figure 3, the server 40 and each of the clients, 60a, 60b and 60c all maintain a persistent or near persistent connection with the central administrative node 50. As in the "Non listening Server" mode, the central administrative node maintains listening ports, which allow the server and other clients to connect to it. Also, as in the previous mode, the central node is addressed preferably by using a domain name, the identity of which the server 40 and all potential clients 60 are aware. Although three clients are shown by way of illustration; any number of clients is possible in this embodiment. In this way, the server and all of the clients are able to communicate with the central node.

Referring to Figure 4, in step B, client 60b wishes to communicate with the server 40. It communicates this request to the central node 50. In step C, the central node 50 processes this request and sends a command to the server 40 to open a listening port which client 60b will later connect to. The central node 50 preferably transmits identifying information to the server 40 which allows the server to correctly distinguish the requesting client from other devices. This identifying information could be any of a number of items, such as the client's IP address, taken singly or in combination. This disclosure does not limit the type of identifying information that could be used. In step D, the server 50 opens the listening port by sending out a request to the client in question and waiting for a response. In step E, the server 50 communicates to the central node 40

that the listening port is open and that the client should connect. In step F, the central node 40 sends a command to the client 60b to connect to the server 50. Lastly, in step G, the client 60b connects to the server 40 via the temporary listening port. The server ensures that this is the device that it expected to connect. If it is not, the request will be immediately rejected and the listening port closed.

Alternatively, the process can be mode to operate with the client opening the temporary listening port. In this implementation, the client is told by the central node in step F to open a temporary listening port and wait for a response from the server. The request from the server in step D would then be accepted by the client and the secure connection is established.

Additional levels of security can be added to the JITL scenario via encryption technology if desired. For example, the messages exchanged in the JITL mode can be encrypted, using algorithms and technologies that are known by those skilled in the art.

As described above, the primary advantage of JITL mode over NLS mode is that a server operating in JITL mode has the ability to provide connections when both the server and the Client are behind firewalls. The primary disadvantage of JITL mode is that it must maintain a connection to a central administrative node.

CLAIMS

1. A method of operating a computer network server in a network having a central node and wherein said network comprises at least one client authorized to access said computer network server via said central node, said method comprising:

accessing said central node;

obtaining the network addresses of said at least one client;

establishing a computer network connection with said at least one client;

receiving a request from said at least one client over said established connection; and

responding to said request.

2. The method of claim 1, further comprising providing a network device, said network device being selected from the group consisting of firewalls, proxy servers, and network translation devices, said network device being in the path between said server and said network.

3. A method of operating a computer network server in a computer network having a central node wherein said network comprises at least one client authorized to access said server, wherein said server has a listening port, accessible during a predetermined time, comprising:

maintaining a connection with a central node;

receiving a command from said central node to open a listening port after said central node receives a request from said at least one client to access said server;

opening said listening port;

sending to said central node instructions for said client to connect to said server over said listening port; and

receiving communication from said client over said listening port after said central node delivers a command to said at least one client to connect to said server.

4. The method of claim 3, whereby said predetermined time is less than one second.

5. The method of claim 3, whereby said server closes said listening port after receipt of said communication.

6. The method of claim 3, whereby said server establishes a network connection with said client after receipt of said communication.

7. The method of claim 3, whereby said server closes said listening port if it receives communication from other than said at least one client.

8. The method of claim 3, whereby said server maintains a persistent network connection to said central node.

9. The method of claim 3, whereby said command is encrypted.

10. The method of claim 3, whereby said instructions are encrypted.

11. The method of claim 3, whereby said communication is encrypted.

12. A method of sharing data between a server and at least one client authorized to access said data resident on said server on a network using network connections, whereby all said network connections between said server and said at least one client are initiated by said server.

13. The method of claim 12, further comprising a central node, whereby said server requests from said central node a list of said at least one clients authorized to access data resident on said server.

14. The method of claim 13, whereby said request is encrypted.

15. The method of claim 13, whereby said server initiates a network connection to each of said at least one authorized clients.

16. The method of claim 15, whereby said at least one authorized client requests data from said server using said network connection previously initiated by said server.

17. A computer system, comprising a central node, a server and at least one authorized client, wherein said server is adapted to access said central node to obtain a list of said clients authorized to access data on said server.

18. The computer system of claim 17, wherein said server is adapted to establish a network connection to each said at least one authorized client.

19. The computer system of claim 18, wherein said server is adapted to receive a request over said established network connection from said at least one client and is adapted to respond to said request.

20. A computer system, comprising a central node, a server and at least one authorized client, wherein said server is adapted to receive notification from said central node that said authorized client wishes to communicate with said server and in response to said notification, is adapted to open a listening port for said authorized client to connect to and sends instructions to said central node to notify said authorized client to communicate to said listening port.

21. The computer system of claim 20, wherein said server is adapted to close said listening port if a device other than said authorized client attempts to communicate to said listening port.

22. The computer system of claim 20, wherein said server is adapted to establish a network connection with said authorized client after said authorized client communicates to said listening port.

23. The computer system of claim 20, wherein said server is adapted close said listening port after receipt of said communication from said authorized client.

24. A computer program product for instructing a processor in a computer network server in a network having a central node and wherein said network comprises at least one client

authorized to access said computer network server via said central node, said computer program product comprising:

a computer readable medium;

first program instruction means for accessing said central node;

second program instruction means for obtaining the network addresses of said at least one client;

third program instruction means for establishing a computer network connection with said at least one client;

fourth program instruction means for receiving a request from said at least one client over said established connection and responding to said request.

25. A computer program product for instructing a processor of a computer network server in a computer network having a central node wherein said network comprises at least one client authorized to access said server, wherein said server has a listening port, accessible during a predetermined time, said computer program comprising:

a computer readable medium;

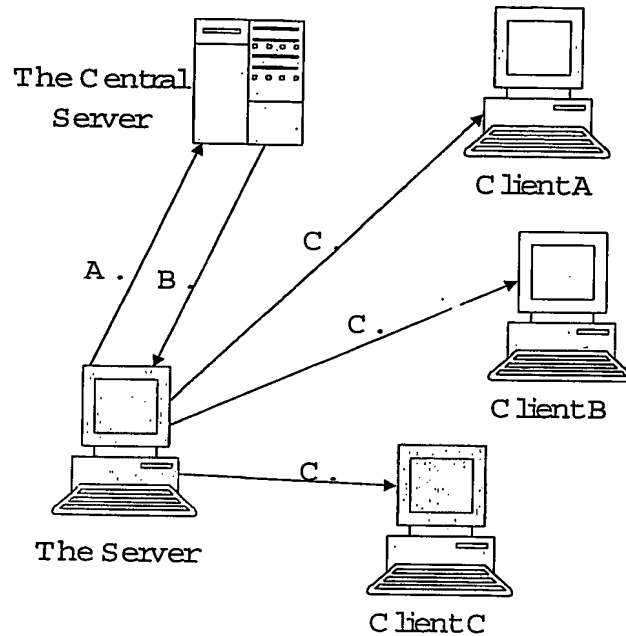
first program instruction means for maintaining a connection with a central node;

second program instruction means for receiving a command from said central node to open a listening port after said central node receives a request from said at least one client to access said server;

third program instruction means for opening said listening port;

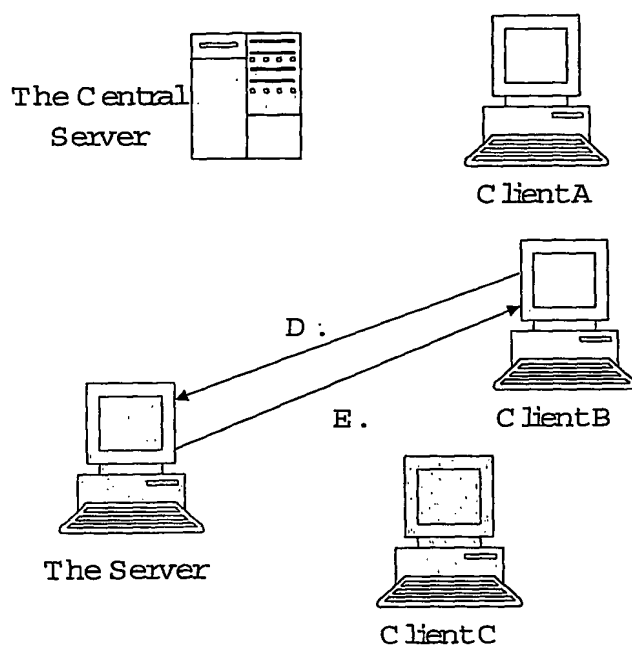
fourth program instruction means for sending to said central node instructions for said client to connect to said server over said listening port; and

fifth program instruction means for receiving communication from said client over said listening port after said central node delivers a command to said at least one client to connect to said server.

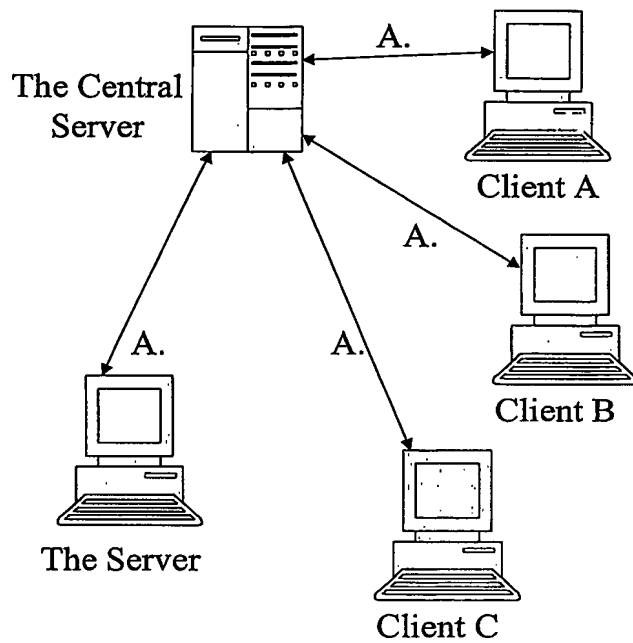
FIG. 1

- A. The server, behind a firewall, router, proxy server or NAT device accesses the Central Server.
- B. The server obtains the IP address of all authorized Clients from the Central Server.
- C. The server then makes a connection with all of the Clients (shown as Clients A, B, and C which are merely representative of any number of Clients).

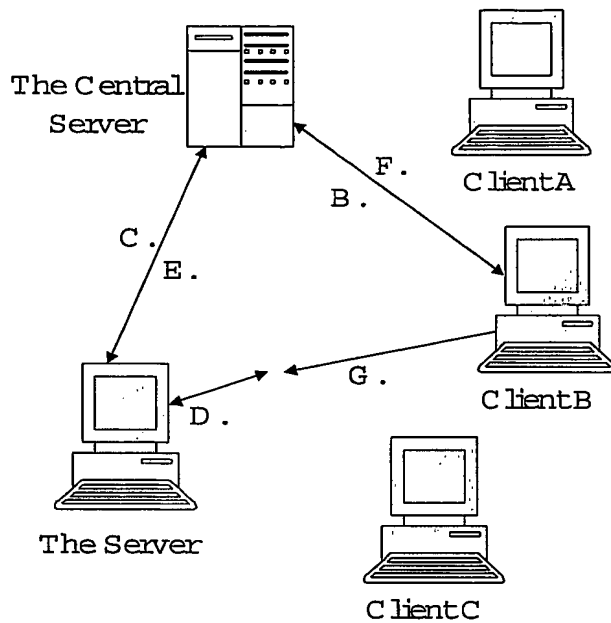
FIG. 2



- D. Exemplary Client "B", using the connection initiated by the server, sends a request for data back to the PDS.
- E. The server then sends the requested content to Client B and waits for the next request.

FIG. 3

A. The server and all Clients maintain a persistent or near persistent connection with the Central Server.

FIG. 4

- B. Client B communicates with the Central Server a request to access the server.
- C. The Central Server sends a command to the PDS to open a "listening" port.
- D. The server opens the listening port by sending out a request and waiting for a response.
- E. The server communicates to the Central Server to have the Client connect.
- F. The Central Server sends a command to the Client to connect.
- G. The Client connects to the server via the temporary "listening" port.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/31333

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 13/00

US CL : 709/200, 203, 208, 225, 227

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/200, 203, 208, 225, 227

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,941,996 (SMITH et al) 24 August 1999 (24.08.1999), entire document	1-25
Y,P	US 6,467,040 B1 (APTE et al) 15 October 2002 (15.10.2002), columns 2-5	1-25
Y	US 5,867,650 (OSTERMAN) 2 February 1999 (02.02.1999), columns 1-3,6,7	1-25
Y,E	US 6,662,228 B1 (LIMSICO) 9 December 2003 (09.12.2003), entire document	1-25
A	US 6,351,772 B1 (MURPHY et al) 26 February 2002, columns 1-5	1-25
A	US 6,163,812 (GOPAL et al) 19 December 2000 (19.12.2002), columns 4-9	1-25
A,E	US 6,712,702 B2 (GOLDBERG et al) 30 March 2004 (30.03.2004), column 30	1,3,12,17,20,24,25

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

16 May 2004 (16.05.2004)

Date of mailing of the international search report

02 JUN 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Ramy Osman

Telephone No. (703) 305-8050

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/31333

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 13/00

US CL : 709/200, 203, 208, 225, 227

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/200, 203, 208, 225, 227

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,941,996 (SMITH et al) 24 August 1999 (24.08.1999), entire document	1-25
Y,P	US 6,467,040 B1 (APTE et al) 15 October 2002 (15.10.2002), columns 2-5	1-25
Y	US 5,867,650 (OSTERMAN) 2 February 1999 (02.02.1999), columns 1-3,6,7	1-25
Y,E	US 6,662,228 B1 (LIMSICO) 9 December 2003 (09.12.2003), entire document	1-25
A	US 6,351,772 B1 (MURPHY et al) 26 February 2002, columns 1-5	1-25
A	US 6,163,812 (GOPAL et al) 19 December 2000 (19.12.2002), columns 4-9	1-25
A,E	US 6,712,702 B2 (GOLDBERG et al) 30 March 2004 (30.03.2004), column 30	1,3,12,17,20,24,25

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

16 May 2004 (16.05.2004)

Date of mailing of the international search report

02 JUN 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Ramy Osman

Telephone No. (703) 305-8050

CORRECTED VERSION

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034190 A2

- (51) International Patent Classification⁷: **G06F**
- (21) International Application Number:
PCT/US2003/031333
- (22) International Filing Date: 2 October 2003 (02.10.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/416,185 4 October 2002 (04.10.2002) US
- (71) Applicant (for all designated States except US): **WOOD-STOCK SYSTEMS, LLC** [US/US]; 36 E. 67th Street, New York, NY 10021 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **HOFFMAN, James** [US/US]; 18 Northwoods Road, Woodstock, NY 12498 (US). **FRISKEL, James** [US/US]; 28 Orange Avenue, Rockledge, FL 32955 (US).
- (74) Agents: **LEMACK, Kevin, S. et al.**; Nields & Lemack, Suite 7, 176 E. Main Street, Westboro, MA 01581 (US).

- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

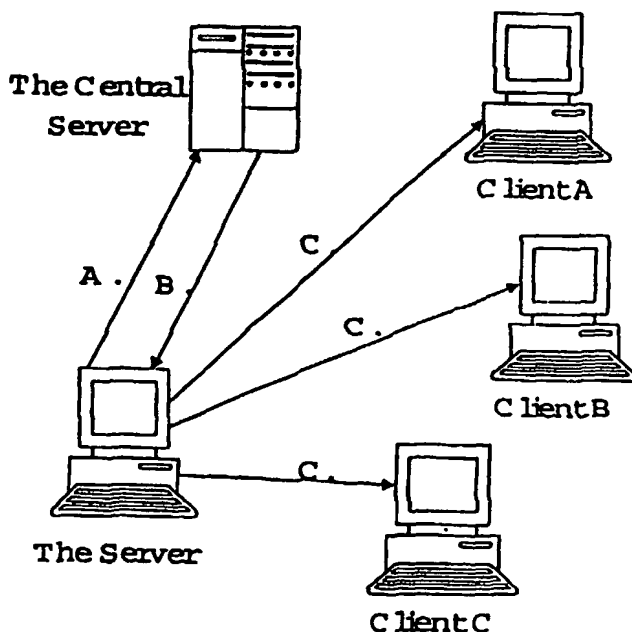
— without international search report and to be republished upon receipt of that report

(48) Date of publication of this corrected version:

10 June 2004

[Continued on next page]

(54) Title: METHOD FOR RUNNING SERVERS BEHIND FIREWALLS, ROUTERS, PROXY SERVERS AND NETWORK ADDRESS TRANSLATION SOFTWARE AND DEVICES



(57) Abstract: The present invention provides a system and method for automatically and securely enabling a server to be accessed by systems and devices under conditions where it would otherwise be inaccessible. Servers maintain higher levels of security as listening ports are not utilized in the invention. The methods described allow access between devices, even in the presence of firewalls, proxy servers and NAT devices.